System Security Plan (SSP) Certification and Accreditation Package (SSPCAP) Requirements Checklist

SSPCAP Requirement [NIACAP System Security Authorization Agreement (SSAA) references are provided as a cross-walk]	**Minimum Content to Satisfy Requirement** [May be in the SSP itself or referenced in the SSP and a full copy appended to the SSP and included in the SSPCAP (or SSAA if used)]	**Included in SSPCAP?**		
		Yes	**No**	**POAM Target Date for Completion**
SECTION A. SYSTEM SECURITY PLAN (SSP)	Is the SSP final and signed by the system owner?			
1 **Define the System** (SSAA Appendices A, B, C, D, and P)				
1.2 System Identification				
1.2.1 System Name/Title	System full name (spell out acronyms), CIO system ID number			
1.2.2 Responsible Organization	Name/address/phone of responsible program office			
1.2.3 Information Contact(s)	Name/title/phone/address of the Designated Approving Authority (i.e., operating unit head or delegated program official), the System Owner, the IT Security Officer, and vendor facility contact (if applicable)			
1.2.4 Assignment of Security Responsibility	Name/title/phone/address of the Information System Security Officer (ISSO), if applicable, or system administrator			
1.3 System Operational Status	State whether the system is under development, operational, or retired. If the system is moving through development phases, include a schedule for the system design, development, implementation, and operational/maintenance status phases.			
1.4 General Description/Purpose	**Detailed** narrative describing what the system is, what it does, the population it serves, and how it fulfills the mission – refer to all associated/related budget documents such as Exhibits 300 and 53 if this is a major system.			
1.5 System Environment	**Detailed** narrative describing where the system is that includes: • A detailed topology graphic that clearly shows ALL the system boundaries and KEY devices within it (Note: this does not require depicting all workstations on every desktop, but you must include all perimeter security devices, firewalls, routers, switches, file/print/application servers, , • A complete listing of all hardware and software (system software and application software) components, including make/OEM, model, version, and service packs. Indicate if software is customized or COTS/GOTS. • A discussion of how it is funded – refer to all associated/related budget documents such as Exhibits 300 and 53. • A discussion of the system location(s) -- whether in a DOC facility or a contractor facility, whether the system is supported/maintained by government or contract staff, and the nature of contract support (if applicable).			

SSPCAP Requirement [NIACAP System Security Authorization Agreement (SSAA) references are provided as a cross-walk]	Minimum Content to Satisfy Requirement [May be in the SSP itself or referenced in the SSP and a full copy appended to the SSP and included in the SSPCAP (or SSAA if used)]	Included in SSPCAP?		
		Yes	**No**	**POAM Target Date for Completion**
1.6 System Interconnection/Information Sharing (SSAA Appendix P)	A **detailed** discussion of its connectivity -- where it goes out and who/what is authorized to come in. Include a discussion of ALL connections to other systems not governed by this security plan, including • Untrusted connections, including connections to the Internet, that require protective devices as a barrier to unauthorized system intrusion. Indicate if the connection is/are government-to-government (G2G), government-to-business (G2B), or government-to-citizen (G2C), etc. and describe the controls to allow and restrict public access. Include in this discussion a description of all perimeter security devices, such as routers and firewalls, and the role these devices play in protecting the system from the untrusted environment (e.g., describe a DMZ set up to protect a web server from malicious Internet traffic and to protect the internal network from the web server to which it is connected if the web server is compromised). • Trusted connections that do not contain barrier protection devices such as firewalls – indicate if G2G, G2B, or G2C, etc., and discuss why the connection is trusted. Reference here and include a full copy in the SSPCAP all Memoranda of Understanding (MOU), Memoranda of Agreement (MOA), and Service-Level Agreements (SLA) for provision of IT security for this connectivity.			
1.7 Sensitivity of Information Handled	Provide a general statement regarding how the drivers for security of the system establish a convincing argument for the "risk of harm" if the system confidentiality, integrity, and/or availability are compromised. How do the sensitivity determinations contribute to the system criticality (business essential, mission critical, or national-critical)? Use criteria as recommended in draft NIST FIPS 199 (at http://csrc.nist.gov/publications/drafts/FIPS-PUB-199-ipd.pdf).			
1.7.1 Laws, Regulations, and Policies Affecting the System (SSAA Appendices A, B, and C if necessary, plus Appendix D)	List by reference ALL applicable regulations, including public laws, federal requirements (e.g., OMB circulars), DOC policies and procedures, and operating-unit specific policies and procedures. Append to the SSP or otherwise include a copy of each in the SSPCAP.			

<table>
<tr><th rowspan="2">SSPCAP Requirement
[NIACAP System Security Authorization Agreement (SSAA) references are provided as a cross-walk]</th><th rowspan="2">Minimum Content to Satisfy Requirement
[May be in the SSP itself or referenced in the SSP and a full copy appended to the SSP and included in the SSPCAP (or SSAA if used)]</th><th colspan="3">Included in SSPCAP?</th></tr>
<tr><th>Yes</th><th>No</th><th>POAM Target Date for Completion</th></tr>
<tr><td>1.7.2 General Description of Sensitivity</td><td>State whether the system’s sensitivity to compromises of confidentiality, integrity, and availability are high, medium, or low – and state WHY. This can be shown in a table format as follows:
<table>
<tr><th>Sensitivity Element</th><th>Sensitivity Rating</th><th>Basis for Rating</th></tr>
<tr><td>Confidentiality</td><td>(High, Medium, or Low)</td><td></td></tr>
<tr><td>Integrity</td><td>(High, Medium, or Low)</td><td></td></tr>
<tr><td>Availability</td><td>(High, Medium, or Low)</td><td></td></tr>
</table>
User accountability can also be addressed as it relates to SSP section 4.1, identification and authentication.</td><td></td><td></td><td></td></tr>
<tr><td colspan="5">**2 Management Controls** (SSAA Appendices G, I, J, and R)</td></tr>
<tr><td>2.1 Risk Assessment and Management (SSAA Appendix G)</td><td>• Provide the control status – in place or planned. If planned, include reference to the POAM action number (e.g., “OU02.5) and state the target completion date.
• Reference that the DOC *IT Security Program Policy*, section 3.1, is followed for risk management, and/or describe other equivalent operating unit specific **methodology** used, such as NIST Special Publication 800-30.
• State whether a system risk assessment was completed, state the date completed (or planned completion), and reference the SSPCAP section containing a copy of the assessment.
• State that the system will be re-assessed for risk upon major system modification or every 3 years (i.e., by completion date + 3 years), whichever date occurs first.</td><td></td><td></td><td></td></tr>
<tr><td>2.2 Review of Security Controls</td><td>Describe briefly or list and append to the SSP or otherwise include in the SSPCAP copies of most recent relevant/applicable audits and assessment reports and last monthly update of detail corrective action Plan of Actions and Milestones (POAM) table for system that addresses audits/reviews). In the SSP:
• Provide the control status – in place or planned. If planned, include reference to the POAM action number (e.g., “OU02.5) and state the target completion date.
• Reference that the DOC *IT Security Program Policy*, section 3.2, is followed for reviews of security controls and/or describe other equivalent operating unit specific methodology used.
• State whether a system self-assessment review was performed in accordance with NIST Special Publication 800-26, state the date completed, and reference the SSPCAP section containing a copy of the assessment. Append to the SSP or otherwise include in the SSPCAP a copy of most recent NIST 800-26 system checklist. State that the system self-assessment will be completed on an annual</td><td></td><td></td><td></td></tr>
</table>

SSPCAP Requirement [NIACAP System Security Authorization Agreement (SSAA) references are provided as a cross-walk]	**Minimum Content to Satisfy Requirement** [May be in the SSP itself or referenced in the SSP and a full copy appended to the SSP and included in the SSPCAP (or SSAA if used)]	**Included in SSPCAP?**		
		Yes	**No**	**POAM Target Date for Completion**
	basis. • State that system vulnerability scanning is performed, specify the systems tested, and the frequency of testing. Include mention of third party contract services to provide this service, or agreements with the DOC CIRT for this service. • State that the system is subject to external audits by OIG and GAO as well as compliance reviews by DOC, and state the date(s) of most recent review(s) for each external party.			
2.3 Rules of Behavior (SSAA Appendix J)	• Provide the control status – in place or planned. If planned, include reference to the POAM action number (e.g., “OU02.5) and state the target completion date. • State whether system Rules of Behavior have been developed and have been distributed to all system users. Describe any requirements for users sign or otherwise acknowledge agreement with the Rules. Append to the SSP or otherwise include in the SSPCAP a copy of the Rules.			
2.4 Planning for Security in the Life Cycle (SSAA Appendix I)	• Provide the control status – in place or planned. If planned, include reference to the POAM action number (e.g., “OU02.5) and state the target completion date. • Reference that the DOC *IT Security Program Policy*, section 3.3, is followed for system life cycle management and/or describe other equivalent operating unit specific methodology used. If a separate document, append a copy of the system life cycle policy that covers all life cycle phases 2.4.1 Initiation Phase 2.4.2 Development/ Acquisition Phase 2.4.3 Implementation Phase 2.4.4 Operation/ Maintenance Phase 2.4.5 Disposal Phase			

SSPCAP Requirement	**Minimum Content to Satisfy Requirement**	**Included in SSPCAP?**		
[NIACAP System Security Authorization Agreement (SSAA) references are provided as a cross-walk]	[May be in the SSP itself or referenced in the SSP and a full copy appended to the SSP and included in the SSPCAP (or SSAA if used)]	**Yes**	**No**	**POAM Target Date for Completion**
2.5 Authorize Processing (include copy of accreditation statement signed by the DAA) 2.5.1 Accreditation Documentation (SSAA Appendix R) 2.5.2 Accreditation Statement (SSAA Appendix R)	• Provide the control status – in place or planned. If planned, include reference to the POAM action number (e.g., “OU02.5) and state the target completion date. • Reference that the DOC *IT Security Program Policy*, section 3.4, is followed for system certification and accreditation and/or describe other equivalent operating unit specific methodology used. • State whether system certification was completed, provide the date completed, and reference the SSPCAP section containing the certification documentation (i.e., Section B of the SSPCAP). • State whether system accreditation was completed and provide the date completed – indicate if full or interim accreditation, or if accreditation was denied. Append to the SSP the accreditation statement, signed by the DAA. The accreditation must be based upon certification testing, and state that the DAA understands and accepts any residual risk of operating the system. The statement may also direct the system owner to take action to further mitigate risk, which must be tracked in the system POAM. • State that the system will be re-certified and re-accredited upon major system modification (as determined by the DAA) or every 3 years (i.e., by completion + 3 years), whichever date occurs first.			
3 Operational Controls (SSAA Appendices K, L, M, N, O, and Q)				
3.MA. Major Application – Operational Controls				
3.MA.1 Personnel Security	• Provide the control status – in place or planned. If planned, include reference to the POAM action number (e.g., “OU02.5) and state the target completion date. • Reference that the DOC *IT Security Program Policy*, section 3.6, is followed for personnel security controls and/or describe other equivalent operating unit specific methodology used. • State whether personnel authorized to bypass system controls (e.g., super-users, system administrators, etc.) have been reviewed for suitability level by the system owner/supervisor, and whether the Office of Security has completed background investigations as required by the *Security Manual*. • Address segregation of duties by specifying the roles and responsibilities for system users and managers and the associated least privileges for each role (e.g., System Owner approves risk assessment and security plan has read/write access to data, ITSO reviews security plans and configuration change forms related to security has read access to security files, DAA authorizes processing, ISSO reviews configuration change forms related to security, System/Network/DB Administrator has read/write/execute). Are job functions rotated? Are vacations or breaks mandated so that another could detect whether inappropriate activities are occurring?			

SSPCAP Requirement	**Minimum Content to Satisfy Requirement**	**Included in SSPCAP?**		
[NIACAP System Security Authorization Agreement (SSAA) references are provided as a cross-walk]	[May be in the SSP itself or referenced in the SSP and a full copy appended to the SSP and included in the SSPCAP (or SSAA if used)]	**Yes**	**No**	**POAM Target Date for Completion**
3.MA.2 Physical and Environmental Protection 3.MA.2.1 Explanation of Physical and Environment Security 3.MA.2.2 Computer Room Example	• Provide the control status – in place or planned. If planned, include reference to the POAM action number (e.g., “OU02.5) and state the target completion date. • Reference that the DOC *IT Security Program Policy*, section 3.7, is followed for physical and environmental controls and/or describe other equivalent operating unit specific methodology used. • Provide a **detailed** narrative of the physical and environmental controls.			
3.MA.3 Production, Input/Output Controls	• Provide the control status – in place or planned. If planned, include reference to the POAM action number (e.g., “OU02.5) and state the target completion date. • Reference that the DOC *IT Security Program Policy*, section 3.8, is followed for production and input/output controls and/or describe other equivalent operating unit specific methodology used. • Provide a **detailed** narrative of the production, and input/output controls.			
3.MA.4 Contingency Planning	• Provide the control status – in place or planned. If planned, include reference to the POAM action number (e.g., “OU02.5) and state the target completion date. • Reference that DOC *IT Security Program Policy*, section 3.9, is followed for contingency planning controls and/or describe other equivalent operating unit specific methodology used. • Provide a **detailed** narrative of the contingency planning policy and procedures. Include procedures for system backup (type and frequency) and tape storage and recycling procedures. Include information about the offsite storage facility. If policy and procedures are not described in this section of the security plan, you must reference and append a separate contingency plan document to the SSP.			
3.MA.5 Application Software Maintenance Controls	• Provide the control status – in place or planned. If planned, include reference to the POAM action number (e.g., “OU02.5) and state the target completion date. • Reference that the DOC *IT Security Program Policy*, section 3.10, is followed for application hardware and software controls and/or describe other equivalent operating unit specific methodology used. • Provide a **detailed** narrative of the application configuration policy (i.e., security settings) and configuration change management procedure for application server hardware, application software, and operating system software. Append as separate document to the SSP if lengthy or complex.			
3.MA.6 Data Integrity/Validation Controls	• Provide the control status – in place or planned. If planned, include reference to the POAM action number (e.g., “OU02.5) and state the target completion date. • Reference that the DOC *IT Security Program Policy*, section 3.11, is followed for data integrity controls and/or describe other equivalent operating unit specific methodology used. • Provide a **detailed** narrative of the data integrity and validation controls (such as			

SSPCAP Requirement [NIACAP System Security Authorization Agreement (SSAA) references are provided as a cross-walk]	**Minimum Content to Satisfy Requirement** [May be in the SSP itself or referenced in the SSP and a full copy appended to the SSP and included in the SSPCAP (or SSAA if used)]	**Included in SSPCAP?**		
		Yes	**No**	**POAM Target Date for Completion**
	virus protection used and how frequently updated). Append as separate document to the SSP if lengthy or complex.			
3.MA.7 Documentation	• Provide the control status – in place or planned. If planned, include reference to the POAM action number (e.g., "OU02.5) and state the target completion date. • Reference that the DOC *IT Security Program Policy*, section 3.12, is followed for system documentation and/or describe other equivalent operating unit specific methodology used. • Discuss the system documentation components and identify the document custodian (e.g., system manuals are maintained by the system administrator; each user has a user manual, etc.). Append as separate document to the SSP if lengthy or complex.			
3.MA.8 Security Awareness and Training	• Provide the control status – in place or planned. If planned, include reference to the POAM action number (e.g., "OU02.5) and state the target completion date. • Reference that the DOC *IT Security Program Policy*, section 3.13, is followed for security awareness, training, and education policy and/or describe other equivalent operating unit specific methodology used. • Provide a **detailed** narrative of the security awareness, training, and education policy and procedures <u>specific to this application</u>. Append as separate document to the SSP if lengthy or complex.			
3.GSS General Support System – Operational Controls				
3.GSS.1 Personnel Controls	• Provide the control status – in place or planned. If planned, include reference to the POAM action number (e.g., "OU02.5) and state the target completion date. • Reference that the DOC *IT Security Program Policy*, section 3.6, is followed for personnel security controls and/or describe other equivalent operating unit specific methodology used. • State whether personnel authorized to bypass system controls (e.g., super-users, system administrators, etc.) have been reviewed for suitability level by the system owner/supervisor, and whether the Office of Security has completed background investigations as required by the *Security Manual*.			
3.GSS.2 Physical and Environmental Protection 3.GSS.2.1 Explanation of Physical and Environment Security 3.GSS.2.2 Computer Room Example	• Provide the control status – in place or planned. If planned, include reference to the POAM action number (e.g., "OU02.5) and state the target completion date. • Reference that the DOC *IT Security Program Policy*, section 3.7, is followed for physical and environmental controls and/or describe other equivalent operating unit specific methodology used. • Provide a **detailed** narrative of the physical and environmental controls.			

SSPCAP Requirement	**Minimum Content to Satisfy Requirement**	**Included in SSPCAP?**		
[NIACAP System Security Authorization Agreement (SSAA) references are provided as a cross-walk]	[May be in the SSP itself or referenced in the SSP and a full copy appended to the SSP and included in the SSPCAP (or SSAA if used)]	**Yes**	**No**	**POAM Target Date for Completion**
3.GSS.3 Production, Input/Output Controls	• Provide the control status – in place or planned. If planned, include reference to the POAM action number (e.g., "OU02.5) and state the target completion date. • Reference that the DOC *IT Security Program Policy*, section 3.8, is followed for production and input/output controls and/or describe other equivalent operating unit specific methodology used. • Provide a **detailed** narrative of the production, and input/output controls.			
3.GSS.4 Contingency Planning (Continuity of Support)	• Provide the control status – in place or planned. If planned, include reference to the POAM action number (e.g., "OU02.5) and state the target completion date. • Reference that DOC *IT Security Program Policy*, section 3.9, is followed for contingency planning controls and/or describe other equivalent operating unit specific methodology used. • Provide a **detailed** narrative of the contingency planning policy and procedures. Include procedures for system backup (type and frequency) and tape storage and recycling procedures. Include information about the offsite storage facility and disaster recovery procedures. If policy and procedures are not described in this section of the security plan, you must reference and append a separate contingency plan document to the SSP.			
3.GSS.5 Hardware and System Software Maintenance Controls	• Provide the control status – in place or planned. If planned, include reference to the POAM action number (e.g., "OU02.5) and state the target completion date. • Reference that the DOC *IT Security Program Policy*, section 3.10, is followed for application hardware and software controls and/or describe other equivalent operating unit specific methodology used. • Describe system configuration policy (i.e., security settings) and configuration change management procedure for system hardware devices, application software, and operating system software. Append as separate document to the SSP if lengthy or complex.			
3.GSS.6 Integrity Controls	• Provide the control status – in place or planned. If planned, include reference to the POAM action number (e.g., "OU02.5) and state the target completion date. • Reference that the DOC *IT Security Program Policy*, section 3.11, is followed for data integrity controls and/or describe other equivalent operating unit specific methodology used. • Provide a **detailed** narrative of the data integrity and validation controls (such as virus protection used and how frequently updated).			

SSPCAP Requirement	**Minimum Content to Satisfy Requirement**	**Included in SSPCAP?**		
[NIACAP System Security Authorization Agreement (SSAA) references are provided as a cross-walk]	[May be in the SSP itself or referenced in the SSP and a full copy appended to the SSP and included in the SSPCAP (or SSAA if used)]	**Yes**	**No**	**POAM Target Date for Completion**
3.GSS.7 Documentation	• Provide the control status – in place or planned. If planned, include reference to the POAM action number (e.g., "OU02.5) and state the target completion date. • Reference that the DOC *IT Security Program Policy*, section 3.12, is followed for system documentation and/or describe other equivalent operating unit specific methodology used. • Discuss the system documentation components and identify the document custodian (e.g., system manuals are maintained by the system administrator; each user has a user manual, etc.). Append as separate document to the SSP if lengthy or complex.			
3.GSS.8 Security Awareness and Training	• Provide the control status – in place or planned. If planned, include reference to the POAM action number (e.g., "OU02.5) and state the target completion date. • Reference that the DOC *IT Security Program Policy*, section 3.13, is followed for security awareness, training, and education policy and/or describe other equivalent operating unit specific methodology used. • Provide a **detailed** narrative of the security awareness, training, and education policy and procedures specific to this general support system. Append as separate document to the SSP if lengthy or complex.			
3.GSS.9 Incident Response Capability	• Provide the control status – in place or planned. If planned, include reference to the POAM action number (e.g., "OU02.5) and state the target completion date. • Reference that the DOC *IT Security Program Policy*, section 3.14, is followed for incident response capability policy and procedures and/or describe other equivalent operating unit specific methodology used. • Provide a **detailed** narrative of the incident response policy and procedures supporting this system environment. Append as separate document to the SSP if lengthy or complex.			
4 Technical Controls (SSAA Appendix N)				
4.MA Major Application Technical Controls				
4.MA.1 Identification and Authentication 4.MA.1.1 Identification 4.MA.1.2 Authentication	• Provide the control status – in place or planned. If planned, include reference to the POAM action number (e.g., "OU02.5) and state the target completion date. • Reference that the DOC *IT Security Program Policy*, section 3.15, is followed for user identification and authentication controls and that the DOC *Policy on Password Management* is followed, and/or describe other equivalent operating unit specific methodology used. • Provide a **detailed** narrative of the policy and procedures for identification and authentication of users to this application. Include a description of technologies used, such as biometrics or smart cards. Append as separate document to the SSP if lengthy or complex.			

SSPCAP Requirement [NIACAP System Security Authorization Agreement (SSAA) references are provided as a cross-walk]	**Minimum Content to Satisfy Requirement** [May be in the SSP itself or referenced in the SSP and a full copy appended to the SSP and included in the SSPCAP (or SSAA if used)]	**Included in SSPCAP?**		
		Yes	**No**	**POAM Target Date for Completion**
4.MA.2 Logical Access Controls (Authorization/Access Controls)	• Provide the control status – in place or planned. If planned, include reference to the POAM action number (e.g., “OU02.5) and state the target completion date. • Reference that the DOC *IT Security Program Policy*, section 3.16, is followed for logical access controls and that the DOC *Remote Access Security Policy* is followed and/or describe other equivalent operating unit specific methodology used. • Provide a **detailed** narrative of the policy and procedures for logical access controls. Include a description of user account configuration (rights and privileges by user group) and configuration policies for security devices and security software (e.g., router, firewall, and RACF settings). Append as separate document to the SSP if lengthy or complex.			
4.MA.3 Public Access Controls	• Provide the control status – in place or planned. If planned, include reference to the POAM action number (e.g., “OU02.5) and state the target completion date. • State whether or not public access is permitted. All statements must be consistent with the narrative provided for section 1.6, S*ystem Interconnection/Information Sharing*. If permitted, provide a **detailed** narrative of the policy and procedures for public access to this system. Describe the controls that allow and restrict public access.			
4.MA.4 Audit Trails	• Provide the control status – in place or planned. If planned, include reference to the POAM action number (e.g., “OU02.5) and state the target completion date. • Reference that the DOC *IT Security Program Policy*, section 3.17, is followed for audit trail policy, procedure, and controls and/or describe other equivalent operating unit specific methodology used. • Provide a **detailed** narrative of the policy and procedures for audit trails, including the log settings, log retention and review policies and procedures, and type of events logged (e.g., all failed logon attempts, all application and operating system software configuration changes).			
4.GSS General Support System Technical Controls				
4.GSS.1 Identification and Authentication 4.GSS.1.1 Identification 4.GSS.1.2 Authentication	• Provide the control status – in place or planned. If planned, include reference to the POAM action number (e.g., “OU02.5) and state the target completion date. • Reference that the DOC *IT Security Program Policy*, section 3.15, and that the DOC *Policy on Password Management* are followed, and/or describe other equivalent operating unit specific methodology used. • Provide a **detailed** narrative of the policy and procedures for identification and authentication of users to this system. Include a description of technologies used, such as biometrics or smart cards. Append as separate document to the SSP if lengthy or complex.			

SSPCAP Requirement	**Minimum Content to Satisfy Requirement**	**Included in SSPCAP?**		
[NIACAP System Security Authorization Agreement (SSAA) references are provided as a cross-walk]	[May be in the SSP itself or referenced in the SSP and a full copy appended to the SSP and included in the SSPCAP (or SSAA if used)]	**Yes**	**No**	**POAM Target Date for Completion**
4.GSS.2 Logical Access Controls (Authorization/Access Controls)	• Provide the control status – in place or planned. If planned, include reference to the POAM action number (e.g., “OU02.5) and state the target completion date. • Reference that the DOC *IT Security Program Policy*, section 3.16, and that the DOC *Remote Access Security Policy* are followed and/or describe other equivalent operating unit specific methodology used. • Provide a **detailed** narrative of the policy and procedures for logical access controls. Include a description of user account configuration (rights and privileges by user group) and configuration policies for security devices and security software (e.g., router, firewall, and RACF settings). Append as separate document to the SSP if lengthy or complex.			
4.GSS.3 Audit Trails	• Provide the control status – in place or planned. If planned, include reference to the POAM action number (e.g., “OU02.5) and state the target completion date. • Reference that the DOC *IT Security Program Policy*, section 3.17, is followed for audit trail policy, procedure, and controls and/or describe other equivalent operating unit specific methodology used. • Provide a **detailed** narrative of the policy and procedures for audit trails, including the log settings, log retention and review policies and procedures, and type of events logged (e.g., all failed logon attempts, all application and operating system software configuration changes).			
SECTION B: CERTIFICATION PACKAGE	Does the SSPCAP contain a complete system certification package (i.e., “yes” to all the following elements)?			
1. NIACAP Work Plan				
1.1 Tailoring Factors 1.1.1 Programmatic Considerations 1.1.2 Security Environment 1.1.3 IT System Characteristics 1.1.4 Reuse of Previously Approved Solutions (for C&A)	Provide a brief narrative for each factor that summarizes and references more detailed information contained in the SSP.			
1.2 Tasks and Milestones	List and describe briefly the major NIACAP tasks and milestones.			
1.3 Schedule Summary	Summarize the NIACAP schedule, list all tasks and milestone (can be in table format).			

<table>
<tr><th rowspan="2">SSPCAP Requirement
[NIACAP System Security Authorization Agreement (SSAA) references are provided as a cross-walk]</th><th rowspan="2">Minimum Content to Satisfy Requirement
[May be in the SSP itself or referenced in the SSP and a full copy appended to the SSP and included in the SSPCAP (or SSAA if used)]</th><th colspan="3">Included in SSPCAP?</th></tr>
<tr><th>Yes</th><th>No</th><th>POAM Target Date for Completion</th></tr>
<tr><td>1.4 Level of Effort</td><td>Calculate the level of effort using Alternatives and Weights, Assurance Ranges, and Certification Types were established by the National Computer Security Center and published in the <i>Certification and Accreditation Process Handbook for Certifiers</i>, NCSC-TG-031, version 1, July 1996.
<b>Table 1. C&A Level of Effort certification weighing factors.</b>
<table>
<tr><th rowspan="2">Security Characteristic</th><th colspan="3">Alternatives and Weights
(based on SSP section 1.7.2)</th><th rowspan="2">Assigned Weight</th></tr>
<tr><th>High</th><th>Medium</th><th>Low</th></tr>
<tr><td>Confidentiality</td><td>w>18</td><td>w>=6 and <18</td><td>w<6</td><td></td></tr>
<tr><td>Integrity</td><td>w>14</td><td>w>=4 and <=14</td><td>w<4</td><td></td></tr>
<tr><td>Availability</td><td>w>17</td><td>w>=5 and <=17</td><td>w<5</td><td></td></tr>
<tr><td>Accountability</td><td>w>14</td><td>w>=4 and <=14</td><td>w<4</td><td></td></tr>
<tr><td colspan="4"><i>Total Weight</i></td><td></td></tr>
</table>
<b>Table 2. C&A Level of Effort certification type determination.</b>
<table>
<tr><th>Assurance Range</th><th>Certification Type</th></tr>
<tr><td>Total of weighing factors <16</td><td>Type 1: Checklist (NIST 800-26)</td></tr>
<tr><td>Total of weighing factors >=16 and <=30</td><td>Type 2: Abbreviated (Type 1 plus system vulnerability scan testing)</td></tr>
<tr><td>Total weighing factors >30 and <=62</td><td>Type 3: Moderate (Type 2 plus system vulnerability scan testing and external penetration testing)</td></tr>
<tr><td>Total weighing factors >62</td><td>Type 4: Extensive (more rigorous than Type 3)</td></tr>
</table></td><td></td><td></td><td></td></tr>
<tr><td>1.5 Roles and Responsibilities</td><td>List the key roles and personnel involved in the certification and accreditation of the system. Include the DAA and their designated representative (if applicable), the system owner, the IT security officer, the System Certifier, and members of the certification team.</td><td></td><td></td><td></td></tr>
<tr><td>1.6 NIACAP Project Plan</td><td>Project schedule, tasks (scope), resources (personnel, cost), and milestones (using MSProject or equivalent)</td><td></td><td></td><td></td></tr>
</table>

SSPCAP Requirement	**Minimum Content to Satisfy Requirement**	**Included in SSPCAP?**		
[NIACAP System Security Authorization Agreement (SSAA) references are provided as a cross-walk]	[May be in the SSP itself or referenced in the SSP and a full copy appended to the SSP and included in the SSPCAP (or SSAA if used)]	**Yes**	**No**	**POAM Target Date for Completion**
2. Security Test and Evaluation (ST&E)				
2.1 ST&E Plan and/or Procedures (SSAA Appendix E)	Provide a **detailed** description of the plan and procedures for the testing of **all** management, operational, and technical controls. This can take the form of a table (such as the NIST SP 800-26 checklist) **supplemented by a test plan or outline**. Include in the ST&E procedure: • list of the tools to be used for internal vulnerability scans and external penetration testing • documents and records to be reviewed • facilities to be inspected			
2.2 Certification Results (SSAA Appendix F)	Provide a narrative summary of the results of all management, operational, and technical control tests. The **summary must be supported** by: • A completed NIST SP 800-26 checklist showing to what maturity level that testing validated the controls. • Copies of all internal vulnerability scan reports and external penetration test logs and results (raw scan and test results). Include all re-scan results performed if initial testing revealed vulnerabilities unacceptable to the system owner – also requires re-inspection of the SSP section 4, *Technical Controls*, to ensure the SSP is updated as necessary to reflect any configuration changes. • Analysis of all internal vulnerability scans and external penetration test logs (can be provided by the CIRT staff or other appropriately qualified personnel).			
2.3 Certifier's Recommendation (SSAA Appendix H)	A memo signed by the System Certifier attesting to the results of certification tests, identifying residual risk not mitigated by adequate controls, recommending specific corrective actions as warranted, and recommendation for either full accreditation, interim accreditation, or to deny accreditation.			